



MINUTES

Identity Theft Prevention Study Committee

December 2, 2008

MEMBERS PRESENT:

Senator Steve Warnstadt, Co-chairperson
Senator Robert M. Hogg
Senator Steve Kettering

Representative Doris J. Kelley, Co-chairperson
Representative Ako Abdul-Samad
Representative Dawn E. Pettengill

MEETING IN BRIEF

.....

Organizational staffing provided
by: Ed Cook, Senior Legal
Counsel, (515) 281-3994

Minutes prepared by: Rachele
Hjelmaas, Senior Legal Counsel,
(515) 281-8127

- I. Procedural Business
- II. Mr. Bill Angrick, Citizens' Aide/Ombudsman
- III. Mr. Bill Brauch, Director, Consumer Protection Division, Iowa Attorney General's Office
- IV. Mr. Richard Varn, Executive Director, Coalition for Sensible Public Records Access (CSPRA)
- V. Ms. Teresa Jennings, Director, State Government Affairs, Reed Elsevier, Inc.
- VI. Mr. Bill Blue, President, Iowa Land Title Association
- VII. Mr. John Gillispie, Chief Information Officer, Information Technology Enterprise, Iowa Department of Administrative Services
- VIII. Iowa Land Records — Ms. Marilyn Dopheide, President, Iowa County Recorders Association, Carroll County Recorder; Ms. Joyce Jense, Chairperson, Electronic Services System, Cass County Recorder; and Mr. Phil Dunshee, Iowa Land Records Project Manager
- IX. Mr. George Davey, Interested Citizen and Privacy Advocate
- X. Committee Recommendations
- XI. Materials Filed With the Legislative Services Agency



Identify Theft Prevention Study Committee

I. Procedural Business

Call to Order. Co-chairperson Warnstadt called the first and only meeting of the Identity Theft Prevention Study Committee (Committee) to order at 9:36 a.m. on December 2, 2008, in the Supreme Court Chamber (Room 103) at the State Capitol.

Committee Business. Upon motion, members of the Committee elected temporary co-chairpersons Warnstadt and Kelley as permanent co-chairpersons of the Committee. The proposed rules for the Committee were approved by voice vote.

Adjournment. The meeting was adjourned at 3:59 p.m.

II. Mr. Bill Angrick, Citizens' Aide/Ombudsman

A. Committee Presentation

Mr. Angrick provided an overview of public record access concerns received from the public by the Citizens' Aide/Ombudsman's Office. He stated that the basic issue is how the government balances the public's right to access records, including electronic records, with a person's expectation that government will not release information making a person who is the subject of that information vulnerable to identity theft. Under Iowa law (Code Section 715A.8), a person commits the crime of identity theft if the person fraudulently uses or attempts to use identification information of another person with the intent to obtain credit, property, services, or some other benefit. Certain identification information can be found on government records because the information is required, requested, or provided gratuitously. Iowa's "Fair Information Practices Act" (Code Section 22.11) requires state agencies to identify the nature and extent of the personally identifiable information collected by the state agency, although the term has never been defined. Upon framing the policy decisions to be considered by Committee members, Mr. Angrick offered the following seven recommendations for the Committee's consideration:

1. Include a specific definition of "personal information" in Iowa's public records law. Mr. Angrick suggested the Committee use the same definition for "personal information" found in the social security breach legislation enacted in 2008 Iowa Acts, S.F. 2308.
2. Give government bodies the authority and discretion to redact certain personal information from a public record. Mr. Angrick suggested the Committee review S.S.B. 1223 from the 2007 Legislative Session relating to the treatment of social security numbers in public records.
3. Iowa law should specify who is authorized to have access to an unredacted version of a public record.
4. Extend the requirements of the "Fair Information Practices Act" (Code Section 22.11), currently applicable only to state agencies, to include local governments.



5. Give government bodies the same authority to charge a flat rate, subscription fee, a per-transaction fee, or a combination of all three for enhanced electronic access, based upon the relevant Pennsylvania law.
6. Amend Iowa public records law to require government bodies to take reasonable precautions when disposing of confidential records or records containing personal information.
7. Establish a permanent Public Records, Open Meetings, and Privacy (PROMP) Advisory Committee based upon Maine law to provide oversight authority necessary to conduct a thorough review of Iowa laws, policies, and practices dealing with Iowa's open meetings and public records laws.

B. Committee Discussion

Committee questions focused on whether the practice of redacting personal information from government records would be a step backwards. Mr. Angrick responded that it would not be a step backwards if the Committee provides clear guidance on what is considered "personally identifiable information" such as that contained in his recommendations. Co-chairperson Kelley raised the issue of how offshore selling of bulk data fits into this discussion and Mr. Angrick agreed this issue needs to be studied further.

III. Mr. Bill Brauch, Director, Consumer Protection Division, Iowa Attorney General's Office

A. Committee Presentation

Mr. Brauch and Ms. Susan Kerr, an investigator from the Consumer Protection Division who specializes in identity theft, presented information relating to the Attorney General's role in preventing and deterring identity theft. Mr. Brauch stated the Consumer Protection Division has participated in many multistate cases involving privacy security breaches by private companies with an emphasis on children's privacy. His division also drafted legislation relating to Iowa's identity theft law and was involved in bills from the 2008 Legislative Session relating to credit freezes and security breach notices.

Mr. Brauch stated the Attorney General's Office performs many functions regarding privacy laws, including handling and storing public documents, advising other government agencies, educating the public, and making policy proposals to the legislature. He further stated that Governor Tom Vilsack's Iowa Privacy Task Force created in October of 2000, which he was a member of, examined the concerns of Iowans with regard to the collection of financial and health privacy information and the use of such information by businesses.

(http://www.idph.state.ia.us/common/pdf/publications/IA_privacy_TF.pdf).

In referencing the final report of the Iowa Privacy Task Force, Mr. Brauch highlighted certain guiding principles formulated by the task force relating to government collection and use of personal financial information. He also cited recommendations contained in a federal government



Identify Theft Prevention Study Committee

privacy task force report reviewing data handling practices by the federal government (<http://www.ftc.gov/os/2008/10/081021taskforcereport.pdf>).

In concluding his remarks, Mr. Brauch stated that the government's information handling practices need to be uniform, reasonable, fair, and understandable. Federal law should serve as the minimum requirement, with Iowa providing greater protection if deemed necessary; however, the level of protection given should not vary by the state agency, county, or city which possesses the data.

Mr. Brauch offered the following six recommendations to the Committee:

1. Ensure that governmental agencies do not post social security numbers, credit card numbers, and other financial account numbers online.
2. Agencies must only ask for social security numbers, credit card numbers, and other financial account numbers if absolutely necessary to deliver a service.
3. Governmental agencies must identify social security numbers, credit card numbers, and other financial account numbers provided voluntarily to ensure they are not made publicly available.
4. Remember that every level and unit of government may possess personal financial information of government employees and must treat that information with great care.
5. Ensure that training on data handling practices is made a part of training for employees in all agencies at all levels of government who handle such information.
6. Finally, policymakers must figure out what government holds in the way of individuals' personal financial data and take reasonable steps to ensure such data is not accessible to the public.

B. Committee Discussion

Co-chairperson Warnstadt questioned whether access to social security numbers and other types of personal information is necessary when pursuing enforcement cases. Mr. Brauch responded that it is critical the Attorney General has access to such information for law enforcement purposes. Committee members and Mr. Brauch agreed the collection and use of personal information requires a delicate balance of collecting only the necessary information to be used for a specific purpose, and not all personal information.

It is difficult to know whether persons who are accessing such personal information are selling such information. Allowing people to "opt in" regarding the collection of personal information is better than "opting out." Mr. Brauch stated that applying restrictions on the sale and resale of personal information can be tricky, as it is important to be able to respond to requests under the open records law, and Iowa law does not inquire as to who requests information and for what purpose that information is requested. The focus should instead be on what information gets into a public record in the first place. The practice of redacting certain personal information is not without error.



Senator Kettering expressed concern about government restrictions on the collection of personal information, the same as restraints on private individuals. Mr. Brauch stated that the law requires the government to be treated the same as a private individual in this regard.

IV. Mr. Richard Varn, Executive Director, Coalition for Sensible Public Records Access (CSPRA)

A. Committee Presentation

Mr. Varn stated that the focus of the discussion should be on the cybercrime industry and the ways in which it monetizes data theft. Although the presentations and discussions so far have focused on redacting personal information from public records, this may not be the most effective way to handle the identity theft issue because of the advancements in cybercrime. He stated that by redacting certain information contained in public records and limiting access to such records, legislators are in danger of fighting the last war against cybercriminals who already have the data and tools they need to commit crimes. Without the ability to uniquely identify the subject of a record, the very people for whom protection is sought will be those most harmed by false positive and false negative findings derived from incomplete and inaccurate public records. This is particularly critical in the current economic climate, as restarting and reforming the credit markets cannot occur without accurate and complete public records to guide decisions.

Mr. Varn further stated that unvalidated, single-factor authentication and a highly evolved and unchallenged cybercrime industry are the primary causes of identity theft, fraud, and crime, not the availability of personal data and access to public records. He noted that the government does not share and validate information, so the private sector is doing it. Using the proper number, kind, and mixture of factors to authorize a person or attribute behaviors to a person is critical to any identity theft discussion, as cybercriminals are faster at adapting their tools than government is in adapting defenses and going on the offensive. There is a desperate need for more cyberpolice and intergovernmental cooperation.

B. Committee Discussion

Senator Hogg asked what Iowans can do to protect against cybercrime. Mr. Varn responded that public education and awareness is a good start, as he might be surprised to learn how many people fall for phishing (an Internet-based technique for obtaining personal information to use for frauds) scams. Co-chairperson Warnstadt questioned how much information cybercriminals actually need to operate. Mr. Varn responded that there are many ways to uniquely identify a person and there are a lot of smart choices a government can make in choosing to collect or not collect certain information.

V. Ms. Teresa Jennings, Director, State Government Affairs, Reed Elsevier, Inc.

A. Committee Presentation



Identify Theft Prevention Study Committee

Ms. Jennings stated that Reed Elsevier, the parent company of a private company called Lexis/Nexis, is the leading provider of information and business solutions to legal, risk management, corporate, government, law enforcement, accounting, and academic professionals. Sources of Lexis/Nexis information include legal, open media, world finance, public data, and international data. Lexis/Nexis information databases are used for many purposes, including but not limited to preventing terrorist activities; locating and recovering missing children; verifying the identity of people; identifying and preventing fraud; preventing and investigating financial crimes; locating heirs and beneficiaries of trusts and unclaimed funds; and locating blood, bone marrow, and organ donors. Ms. Jennings provided three scenarios as examples of how Lexis/Nexis databases help prevent identity theft and fraud.

B. Committee Discussion

Committee members questioned what percentage of banks and retail stores actually use services such as those provided by Lexis/Nexis. Ms. Jennings responded that under the requirement of the USA Patriot Act, financial institutions must, among other requirements, establish procedures for identifying customers opening accounts, including procedures to verify customer identity and maintaining records of information used to verify identity. Representative Abdul-Samad questioned how many other companies perform the same services as Lexis/Nexis and whether such companies are vulnerable to a data breach. Ms. Jennings responded that companies such as Lexis/Nexis are unique, but do exist, although many companies only provide information in certain specific areas, such as background checks. She also stated that Lexis/Nexis was the subject of a data breach in 2005, but that the company took all the appropriate steps to repair the breach for affected customers, including providing notices, tracking, free credit monitoring, and credit insurance.

VI. Mr. Bill Blue, President, Iowa Land Title Association

A. Committee Presentation

Mr. Blue, who also represents abstractors, stated that the Iowa Land Title Association (association) opposes online land records (Iowa Land Records) because of the concern that out-of-state title insurance agents writing business on an Iowa property can sell a title policy that an Iowa abstractor cannot and such out-of-state agents can bypass doing business with anyone in Iowa. He stated the bulk sale of data hurts Iowa's land title system and encourages capital flight from the state-operated title guaranty program.

If Iowa Land Records (ILR) does continue to operate, the Association favors a subscription-based system assessing a cost to users to pay fees associated with building and maintaining such an online database to ensure a secure system. He also recommends that a tracking system be put in place to identify system users. The association also opposes charging a fee to everyone who files a document to build, fund, and maintain the online database. The association supports restricting access to online records to persons who have a legitimate business need to access such records.

B. Committee Discussion



Co-chairperson Kelley expressed concern about the availability of a backup source of information in case of a disaster if land records are not online. Mr. Blue responded that all abstract companies have computerized records now. He cautioned against complete reliance on the online system in order to complete a title plan, as some records are kept by names and not by the description of the real estate.

VII. Mr. John Gillispie, Chief Information Officer, Information Technology Enterprise, Iowa Department of Administrative Services

Committee Presentation

Mr. Gillispie stated that public records custodians need to be very sensitive to the public's expectation that government will protect people's personal data, and the dilemma for public records custodians is balancing the competing interests of individual privacy in such personal data with the public's need for disclosure of public information. The public's need for disclosure was not as pressing an issue 10 years ago as it is now in the digital age, as years ago, public records existed in "practical obscurity;" although such records were open and available for public access, the public actually had to physically go to a government building and figure out how to access the records. Electronic access to records has changed all this. The difficulty is keeping sensitive personal information out of the hands of identity thieves while allowing businesses and government sufficient means to accurately identify people. In particular, government should eliminate the unnecessary use and disclosure of social security numbers as an identifier whenever possible.

In light of the foregoing, Mr. Gillispie offered the following identity theft preventive measure recommendations for government records custodians:

1. Adopt a privacy policy that includes responsible information handling practices.
2. Appoint a knowledgeable individual to be responsible for the privacy policy.
3. Store sensitive personal data in secure computer systems.
4. Store physical documents in secure spaces such as locked or access-controlled cabinets.
5. Dispose of documents properly.
6. Build appropriate document destruction capabilities into the office infrastructure.
7. Conduct regular staff training.
8. Conduct privacy walk-throughs and make spot checks on proper information handling.
9. Limit data collection to the minimum information needed.
10. Limit data displays and disclosure of social security numbers and other sensitive information.



Identify Theft Prevention Study Committee

11. Restrict data access to staff with a legitimate need to know.
12. Safeguard mobile devices that contain sensitive personal data.
13. Notify constituents and employees of computer security breaches involving sensitive personal information in compliance with Code Chapter 715C.
14. Develop a response plan to be used if sensitive employee or constituent data is lost, stolen, or inappropriately acquired electronically.

VIII. Iowa Land Records — Ms. Marilyn Dopheide, President, Iowa County Recorders Association, Carroll County Recorder; Ms. Joyce Jense, Chairperson, Electronic Services System, Cass County Recorder; and Mr. Phil Dunshee, Iowa Land Records Project Manager

A. Committee Presentation

Mr. Dunshee presented a brief history of the ILR, the source for electronic information relating to recorded real estate documents in Iowa. Mr. Dunshee noted that the purpose of the County Land Record Information System (CLRIS) established in 2005 legislation was to create a statewide land record indexing and imaging database, to make land record information accessible through the Internet, and to enable electronic submission of documents for recording purposes. The ILR website was launched in January of 2005, providing electronic access to real estate land records filed with county recorders and is currently operated pursuant to a Code Chapter 28E agreement with all counties in Iowa.

Mr. Dunshee stated that issues arose early in 2008 that some of the electronic records contained images of documents containing personal information such as social security numbers and bank, credit, and debit card numbers. As a result, although the electronic submission service is fully operational, access to the image repository on the ILR website has been restricted and the examination of land records occurs at the county courthouse. As a result of the decision to limit access to much of the information on the website, ILR is pursuing a request for proposals for image redaction services. In addition, the legislative considerations and options being explored to ensure future access and to clarify the duties and responsibilities of county recorders relative to public web access to real estate records are as follows:

1. While current law prohibits document preparers from including personally identifiable information in real estate documents and requires recorders to have a redaction procedure in place, recent concerns indicate that a more comprehensive redaction process is expected. Additionally, recorders have expressed some uncertainty about their statutory authority to redact information from real estate documents and about whether all or a portion of personally identifiable information should be redacted. An amendment to Code Section 331.606A may help clarify these issues.



2. Recorders in many counties have previously taken the initiative to redact social security numbers from real estate documents. As additional steps are taken to redact personally identifiable information from electronic documents, it is important that unaltered versions of each document be archived in the event that it is necessary that the personally identifiable information be accessible to authorized persons or organizations.
3. Recorders and other county officials have been required to provide open access to records housed in the courthouse or other county administrative facilities. The “golden rules” of public records have required recorders to provide access to records without restrictions. While privacy activists have recommended that access to any record with personally identifiable information be restricted, there could be substantial cost and service disruption if redaction requirements are applied to documents archived in traditional formats such as paper or microfilm. Legislation may be needed to clarify that individuals may continue to view and copy records when visiting the office of the county recorder.
4. If a comprehensive redaction process is implemented, county recorders and the governing body for CLRIS may desire protection from liability for redaction errors.
5. Legislation may be needed to clarify the authority to sell land record files, especially as it relates to providing external organizations with access to real estate records in “bulk” or batch electronic files.
6. During the five years since the enactment of the original enabling legislation for CLRIS, many structures and policies have been established under a Code Chapter 28E agreement among the participating counties. It would be beneficial to have some of these structures and policies codified to ensure the long-term success of the system.
7. Redaction processes and the reconfiguration of the image repository and operating system may be needed to ensure the protection of personally identifiable information. Costs for these activities and for resources needed to ensure the long-term sustainability of the system need to be considered and options to secure the necessary funding must be explored. In the absence of additional resources, the system will continue to operate with access to index information only, maintenance of electronic submission services, and incremental improvements to basic functions. Possible options include an increase in the electronic transaction fee under Code Section 331.605C, authorization to reconfigure the system as a subscription service similar to the Iowa Court Information System, or both.

B. Committee Discussion

Co-chairperson Kelley questioned whether it would make more sense if every county had access through an area wide network so there is only one entity redacting personal information instead of individual counties redacting the information. Mr. Dunshee responded that if the ILR decides to pursue a redaction procedure, it would be implemented in a uniform manner.



Identify Theft Prevention Study Committee

Co-chairperson Kelley queried whether Mr. Dunshee could utilize the Iowa Communications Network to aid in monitoring the security of the system. Mr. Dunshee responded he would utilize it if he could and that the system is very secure.

Representative Pettengill stated that many constituents express concern about the criteria used to become a member with access to the land records. Mr. Dunshee responded that up until access was restricted in late October 2008, the registration to become a member involved a self-registration process which has been revised to require the true identity of the users.

IX. Mr. George Davey, Interested Citizen and Privacy Advocate

Mr. Davey presented an array of highly personal information including personal signatures he obtained on others simply by downloading information from the Internet. He stated he obtained social security numbers and personal credit information from many sources including the Linn, Sac, Polk, and Lee county recorders' websites. He stated that redaction does not work because many attempts to redact information are performed in a careless manner and are not uniform. There should be some sort of an informed consent procedure so consumers can allow or disallow the release of certain personal information. Posting social security numbers in public records should subject a person to criminal sanctions and people who locate others' personal information should receive an award.

X. Committee Recommendations

The Committee made the following recommendations:

1. Iowa's public records law needs to define the term "personal information" and should consider using the definition for "personal information" found in the security breach legislation that is codified at Code Section 715C.1(11).
2. Iowa law should give government bodies the authority and discretion to redact certain personal information from a public record.
3. Iowa law should specify who has access to view unredacted versions of public records.
4. State agencies should regularly review and determine compliance with Code Section 22.11, the "Iowa Fair Information Practices Act," and Iowa law should extend these requirements to local governments.
5. Government bodies should be given the authority to charge a flat rate, a subscription fee, a per-transaction fee, or a combination thereof for "enhanced electronic access" to public records.
6. Government bodies should be required to take reasonable precautions when disposing of confidential records or records containing personal information.
7. A permanent Public Records, Open Meetings, and Privacy (PROMP) Advisory Committee should be created to serve as a resource for ensuring compliance with Iowa



laws dealing with public records and open meetings, including but not limited to Code Chapters 21 and 22, referred to as "freedom of information laws."

8. Government agencies should not ask for and make available personal information, including social security numbers, credit card numbers, and other financial account numbers, unless having established reasons as to why the information is absolutely necessary.
9. County recorders should have a duty to preserve an unaltered version of each document they record, but should also have the duty to redact personal information on documents made generally available to the public.
10. Offshore entities should be restricted from accessing government records that contain unredacted social security numbers.
11. Consideration should be given to creating an areawide network connecting all governmental entities with one entity solely responsible for redacting personal information and the dissemination of all electronic documents.

XI. Materials Filed With the Legislative Services Agency

The following materials listed were distributed at or in connection with the meeting and are filed with the Legislative Services Agency. The materials may be accessed from the <Additional Information> link on the Committee's Internet website:

<http://www.legis.state.id.us/aspx/Committees/Committee.aspx?id=238>.

1. [William Angrick, Citizens' Aide/Ombudsman—Committee Presentation.](#)
2. [William Angrick, Citizens' Aide/Ombudsman—Summary of Recommendations.](#)
3. [William L. Brauch, Director, Consumer Protection Div., AG—Comments.](#)
4. [Richard Varn—Committee Presentation.](#)
5. [Richard Varn—Eugene Kaspersky—The Cybercrime Arms Race.](#)
6. [Richard Varn—CSPRA—Social Security Numbers, Public Records, and Identity Theft — Just Say "No" to Redaction.](#)
7. [Richard Varn—CSPRA—SSN's in the Private Sector—Comment.](#)
8. [Richard Varn—MessageLabs—The Online Shadow Economy.](#)
9. [Richard Varn—Computerworld Security—Article.](#)
10. [Teresa Jennings—Lexis/Nexis—Committee Presentation.](#)
11. [John Gillispie—DAS—The Records Custodians Dilemma—Public Records vs. Personal Privacy.](#)



Identify Theft Prevention Study Committee

12. [Bill Blue—Iowa Land Title Association—Key Points.](#)
13. [Bill Blue—Iowa Land Title Association—Data Tree, LLC Integration Agreement.](#)
14. [Iowa Land Records—Committee Presentation.](#)
15. [Iowa Land Records—Legislative Options.](#)
16. [George Davey—Committee Presentation.](#)
17. [Background Information, Ed Cook, LSA Legal Services.](#)
18. [Cate and Varn, The Public Record: Information Privacy and Access.](#)
19. [Iowa Land Records—Stakeholder Presentation.](#)
20. [PRIA—Privacy and Public Land Records.](#)
21. [PRIA—State Redaction Laws.](#)
22. [Social Security Numbers and County Recorders—Attorney General Opinion.](#)

3720IC